International Journal of Security and Its Applications
Vol.8, No.3 (2014), pp.39-48
http://dx.doi.org/10.14257/ijsia.2014.8.3.05

SSM: Secure Service Manager for the Internet of Things

Jiye Park and Namhi Kang*

Digital Media Department, Duksung Women's University, Seoul, Korea
jiyepark@duksung.ac.kr, kang@duksung.ac.kr

Abstract

Internet of Things (IoT) has attracted attention in various fields where small devices such as sensors and actuators are intended to be connected with each other by using TCP/IP protocols. To build value-added services in such fields, security is one of the most important considerations. The IETF standard group has proposed to use the DTLS protocol to provide security services with constrained devices in lossy networks. However, the protocol cannot cover all constrained devices because of heterogeneous properties. Under the respect, we propose a secure IoT architecture and design a secure service manager (SSM) that is motivated by traditional web service architecture.

Keywords: *Internet of Things, Web of Things, Security, Datagram TLS*

1. Introduction

Lots of devices are recently becoming smart thanks to the decreasing cost of chips and the advances in wired and wireless communication technologies. In addition, the devices are intended to connect with each other and further connect to the Internet by using TCP/IP protocol suites. Thereby high-power computing systems can be linked with small devices directly to realize physical mash-up services. Also, small devices can use the high computing power of the systems anytime, anywhere. The popularization of smart devices and the expansion of wireless communications coverage have introduced new social paradigm in which people own and use several smart devices. There are now approximately 10 billion objects connected to the Internet, and this number is expected to increase to 16 billion by 2020 [1]. IoT, one of the most highlighted internet technologies, can provide various services through such connected things.

IoT can be applied to many traditional industrial fields including home automation systems, building automation systems (BASs), smart healthcare systems, and others. In these fields, many applications are required to support security and privacy. More specifically, data confidentiality, availability, integrity, and authenticity must be ensured. However, there are several issues. Most of all, device resources are generally constrained and a communication channel is regarded as low-power and lossy networks (LLNs). In many scenarios, limited resources make it difficult for devices to compute cryptographic primitives efficiently. Previous studies have examined several security schemes suited for sensor networks, but it is difficult to directly apply such schemes to IoT. In sensor networks, communication entities are generally protected within a closed network. By contrast, IoT entities are connected to the Internet such that data is transferred over the global and public Internet. Consequently, this entails much more threats and vulnerabilities [2].

* Corresponding author: kang@duksung.ac.kr

ISSN: 1738-9976 IJSIA

The capability of end systems used on the Internet has improved rapidly, but embedded systems are less affected by Moore's law than internet devices [3]. Resources of IoT devices, such as CPUs, memory, and batteries, are highly constrained. In addition, the reliability of data packets cannot be guaranteed because networks are LLNs such as IEEE 802.15.4. For these reasons, there is a need to consider additional problems that are not applicable to the Internet.

To consider differences in device performance, the IETF Light-Weight Implementation Guidance (LWIG) working group classifies devices into three classes (classes 0 to 2) based on their capability [4]. In particular, devices containing a data storage capacity (*i.e.*, RAM) less than 10 KiB and a code size (i.e., flash memory) less than 100 KiB belong to class 0. The IETF Constrained RESTful Environment (CoRE) working group standardizes the constrained application protocol (CoAP) for resource-constrained devices. The CoAP is a lightweight version of HTTP protocol. And several security protocols such as IKEv2, PANA, TLS, HIP, and EAP have been considered for IoT devices [5].

Because CoAP runs over UDP, Datagram Transport Layer Security (DTLS) is being discussed as a standard for the IoT security protocol. However, DTLS is too heavy for highly constrained devices in classes 0 and 1. In addition, the DTLS handshake message reduces LLN performance. In this regard, lightweight DTLS has been proposed (see Section 2 in detail), but some problems remain. First, highly constrained devices in class 0 still cannot use lightweight DTLS. Second, it has low scalability, especially when a CoAP client wants to communicate with several sensors (i.e. 1:N DTLS connections). When a client communicates with many devices, it has to create a DTLS connection per each of the devices. Third, it might not be practical in some scenario consisting of heterogeneous devices having different capabilities. These motivate us to propose a secure IoT architecture [2].

The rest of this paper is organized as follows. Section 2 provides related work. Section 3 describes an alternative IoT system architecture. In Section 4, we presents use cases to show applicability of the proposed model. Then we conclude in Section 5.

2. Related Work

The DTLS protocol provides secure communication with UDP-based applications as TLS does for TCP-based applications. The IETF CoRE working group has mandated to use DTLS as a default secure scheme for CoAP in the IoT system. Three issues have to be considered to apply the DTLS protocol. First issues is the end-to-end (E2E) security problem in case of TLS/DTLS mapping. Second, DTLS cannot support legacy sensors that do not support CoAP and constrained devices categorized in classes 0 and 1. Third, DTLS handshake message flights are too heavy to use in LLNs. To cope with these problems, DTLS in the constrained environment (DICE) has recently been registered as an IETF working group. Nevertheless, performance differences between devices have yet to be considered.

In IoT, smart devices in LLNs might to be connected with systems in the Internet. Therefore, mapping of CoAP/DTLS to/from HTTP/TLS must be considered. The 6LoWPAN border router (6LBR) or proxy server can be used to interconnect the LLN with the Internet and performs the mapping between TLS and DTLS. During this process, E2E security can be broken. As a solution, the DTLS capsulation for support E2E security has been proposed [6], where CoAP messages, DTLS information with the end node, and the UDP and IP of the end node are included in application data. Then the DTLS, UDP, and IP of 6LBR are included in each layer. The scheme interconnects two different networks by using a secure tunnel, but it not only causes a lot of overhead in the LLN but also requires many changes in protocol. In this regard, a fully implemented two-way authentication security scheme has been proposed [7]. In the scheme, the Trusted Platform Module (TPM) is used to provide an E2E two-way authentication channel. Devices are separated depending on whether the TPM is included. Devices including the TPM perform a fully authenticated handshake with the CoAP client. Other devices use a protokey to derive the PSK for the DTLS handshake. However, this requires 18 KiB RAM and 63 KiB ROM and thus is not suitable for constrained devices categorized in classes 0 and 1.

To reduce code size for constrained devices, tinyDTLS based on Contiki OS has been proposed [8]. But the tinyDTLS is still heavy for constrained devices in classes 0 and 1 since it requires 11 KiB RAM and more than 77 KiB ROM. To reduce more, a modified tinyDTLS version has been implemented in [9] for devices categorized in class 1. However, there is a limitation in that it must use only a symmetric key.

The DTLS protocol has six message flights during the handshake phase. Thus, a single loss of message leads to restarting the handshaking process again. Packet delay and loss can be frequently happen in LLNs. In addition, performance of constrained devices can be degraded because of the reordering process. These result in difficulty in adopting DTLS protocol to IoT devices. As an alternative approach, certificate based authentication system for IoT has been proposed [10]. In the approach, a gateway verifies the certificate using OCSP to reduce computational complexity. However, the trust of gateway is a concern because certificate is verified by the gateway.

3. Proposed Security Architecture

The proposed system is motivated by a conventional web service architecture based on TCP/IP networks. Web architecture is generally divided into front-end and back-end parts. Web client (*i.e.*, browser) and web server are included in the front-end part. On the other hand, web processes, database, and authentication server are in the back-end part as shown in Figure 1.

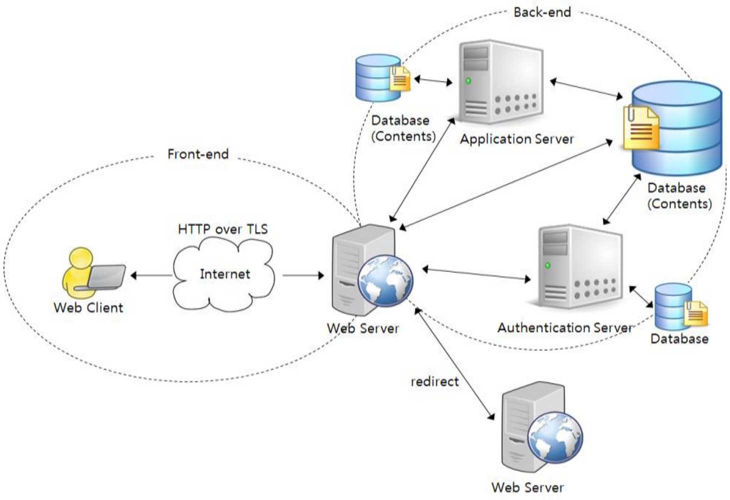


Figure 1. Web Service Architecture

A client usually relies on SSL/TLS sessions connected to web server to protect data securely. Note here that the client just consider a secure session between him and the web server (*i.e.*, front-end part). He does not deeply consider about the security of the back-end part. For example, when the client receives data from the database server via the web server, the client does not care about the security between web server and database system.

Generally, the client believe that the web server get the data from database securely. That is, even when there is no direct TLS connection between the client and the database server, E2E security is not generally assumed to be broken.

The back-end system is constructed depending on the properties of a service such as the number of clients, required infrastructure and others. In case of a small web service system, different types of servers might be built in a single server, and contents are protected by internal security protocols. Physical and logical security is applied to large web service systems. Even when the client clicks the link to the web server in another domain, the web server redirects it to the other web server, and a new TLS connection is created between the client and the other server.

The IoT service shares many similarities with such a web service. Therefore, scalability, practicality, and security can be inherited to IoT/WoT services. Figure 2 shows the proposed architecture for supporting secure IoT services. Similarly to traditional web service architecture, IoT domain can be classified into front-end and back-end parts. The CoAP client and the secure service manager (SSM) are included in the front-end part, and the application server and many heterogeneous sensors come under the back-end part.

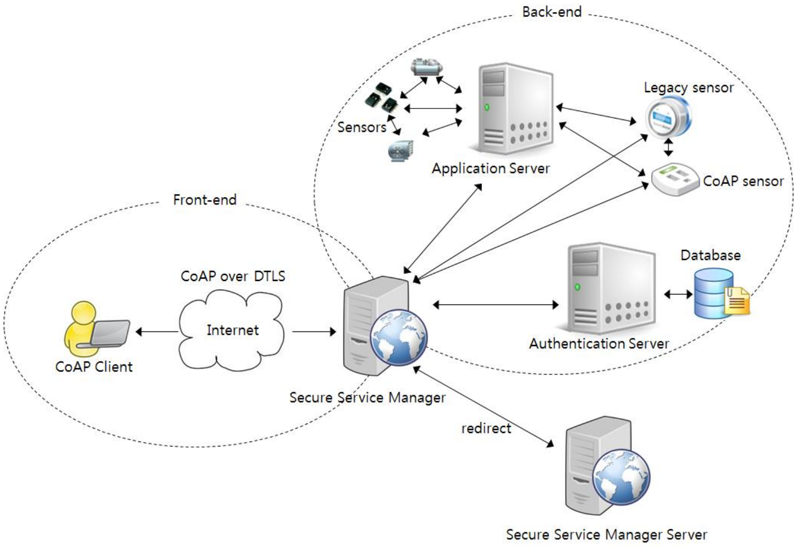


Figure 2. Proposed IoT Service Architecture

In the proposed architecture, a CoAP device (*i.e.*, end thing) is not a physical system but data (*i.e.*, a content of web services such as html file or image file). Also, the CoAP server or proxy is regarded as a infrastructure device like an application server in web service. Thus role of the SSM is similar to the web server in traditional Internet. For example, a smartphone can be a SSM in a personal healthcare service.

A client can request a DTLS connection to the SSM by using CoAPs. Then, lightweight DTLS methods can be used for building DTLS connections between the CoAP client and the SSM. When the CoAP client wants to get data from the CoAP sensor, the end node of this communication is not the sensor having data but the SSM. Therefore, there is no end-to-end security problem. In the back-end system, various security protocols can be applied between the SSM and sensors depending on the performance of each sensor and the importance of sensed data. As a result, both legacy and CoAP devices can communicate with each other securely by using the secure manner regardless of presence of DTLS connection.

4. Use Cases

The proposed system architecture is secure, scalable, and practical so that it can be applied to various scenarios in IoT services. This section presents smart health care service and building automation system as the applicable scenarios.

4.1. Smart Health Care Service

Smart sensors used in health care system can contain sensitive and private information so that high level security is required. But the problem is that health care sensors are very resource constrained (*e.g.*, Texas Instrument MSP430 has 60 KiB flash memory and 2 Kib RAM). Besides, the sensors are moving from space to space. Therefore, static DTLS connection between a client and each sensor is not suitable for Body Area Network (BAN).

In smart health care services, sensor can be operated as a client and a server as well depending on the scenario. If a CoAP client outside of BAN requests data to SSM and then SSM requests data to a sensor, sensor in BAN is a CoAP server. In this case, the CoAP client and the SSM are regarded as devices in the front-end part. Therefore, a connection of the CoAP client is thus ended at the SSM. Note that smart health care sensors generally send data periodically to server. Thus we focused on the following cases (see Figure 3).

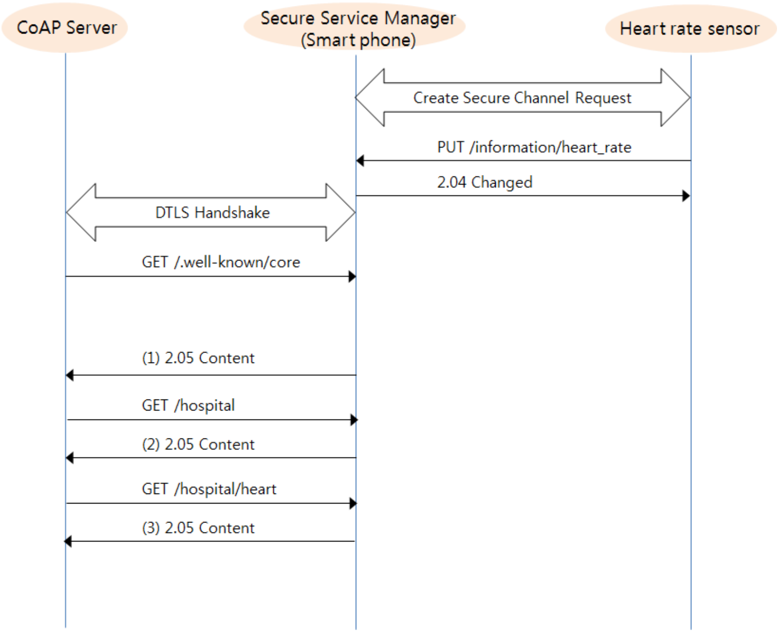


Figure 3. Message Transaction for Health Care System

In Figure 3, transaction message format have the following format.

(1) </exercise>;ct=10, </hospital>; ct=11, </settings>; ct=12
(2) </information/heart_rate> ;if=”information”,
</information/blood_pressure>; if=”information”
(3) Data of the heart_rate sensor

We use a smart phone as a SSM. Before sending sensitive information from the health care sensors, sensors can request to initiate secure channel according to a pre-defined security protocol between the sensors and the SSM. As mentioned in Section 3, security protocol can be pre-defined according to the sensor performance and security level of information. This is similar to the policy of traditional web service. After this, a CoAP client (outsider) requests DTLS connection to SSM. Because owner of the SSM and the sensors in BAN is the same service provider, the CoAP client can believe SSM. If DTLS connection is successfully constructed, the CoAP client sends a GET method to the SSM. Then, the SSM sends back a response message about directory information (1). In order to check the status of the patient, the CoAP client requests body status information. Now, the SSM responds to the request (2). After this, the CoAP client requests heart rate data and the SSM sends the data of heart rate (3). This is almost the same to a web service system. In this way, sensors in BAN and CoAP server can communicate securely via the SSM.

4.2. Building Automation System

Temperature, light, security, and energy sensors, among others, are deployed everywhere in a building. If there are 10 light sensors on each floor and the building has 10 floors, then the building has 100 light sensors. To securely change the setting for light sensors, 100 DTLS connections are needed. This sharply reduces the scalability of the BAS. Figure 4 shows the BAS scenario in which the SSM is used.

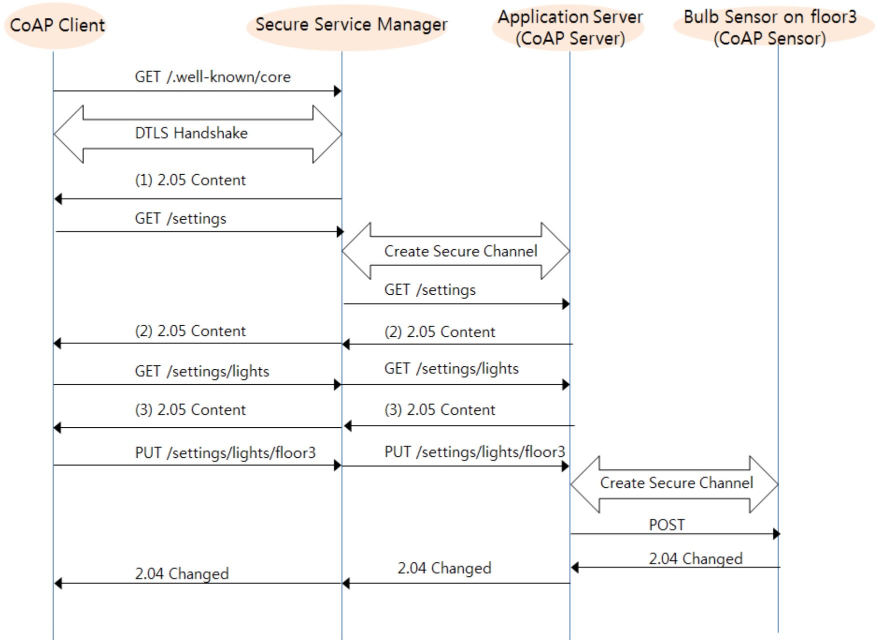


Figure 4. Message Transactions for BAS

The CoAP client sends initial request message including /.well-known/core and creates a secure tunnel with the SSM by using the DTLS protocol. If the secure channel is successfully created, then the SSM sends information on the placement of grouped sensors to the CoAP client (1). Here the CoAP client sends a message about settings for light sensors grouped as a single content to the SSM. Then the SSM sends the message received from the CoAP client to the application server after creating a secure channel which is created by a predefined manner. The application server responds to that request, and the SSM sends a message to the CoAP client (2). The CoAP client requests information on subfolders. When the CoAP client receives sensor information on each floor (3), it sends a command to light sensors on the third floor. If the command is passed through the SSM, then the application server creates a secure channel with each light sensor on the third floor. After the secure channel is created, the application server sends the command to each light sensor. When the application server receives a response from each sensor, it sends results to the SSM. Finally, the SSM responds to the CoAP client. Because each light sensor is grouped together logically, the client needs no DTLS connection to each sensor. Therefore, our proposed model based on the SSM can enhance the scalability of large systems such as BAS.

In Figure 4, the message format denoted by each number in parenthesis among transaction messages is as follows respectively.

(1) </settings>;ct=20, </controls>;ct=21
(2) </settings/lights>;if=”settings”, </settings/security>;if=”settings”
(3) </settings/lights/floor1>;if=”lights”, </settings/lights/floor2>;if=”lights”,
</settings/lights/floor3>;if=”lights”

5. Conclusion

In this paper we propose an alternative system model that provides security, scalability, and practicality for IoT services in which the SSM is the major entity. Through the proposed model, resource-limited sensors such as those in classes 0 and 1 can communicate with the CoAP server or client in a secure manner with no direct DTLS connection. We also present an applicable scenario, where the proposed architecture is well suited and practical for IoT based service.

Acknowledgements

This research was supported by the MSIP(Ministry of Science, ICT&Future Planning), Korea, under the ITRC(Information Technology Research Center)) support program (NIPA-2013-H0301-13-1003) supervised by the NIPA(National IT Industry Promotion Agency).

References

[1] H. Zhou, “The Internet of Things in the Cloud”, CRC Press Taylor & Francis Group, **(2013)**.

[2] J. Park and N Kang, “Designing a Secure Service Manager for Internet of Things”, Proceedings of the 2013 International Workshop on Multimedia, Jeju Island, Korea, **(2013)** December 11-13.

[3] H. Tschofenig and J. Arkko, “Report from the Smart object workshop”, IETF Request For Comments, vol. 6574, **(2012)**.

[4] C. Bormann and M. Ersue, “Terminology for Constrained Node Networks”, IETF Internet-Draft, **(2013)**.

[5] O. Garcia-Morchon, S. Keoh, S. Kumar, R. Hummen and R. Struik, “Security Considerations in the IP-based Internet of Things”, Internet-Draft, Internet Engineering Task Force, **(2013)**.

[6] M. Brachmann, S. Keoh, O. Morchon and S. Kumar, “End-to-end Transport Security in the IP-based Internet of Things”, Proceedings of the 21st International Conference on Computer Communications and Networks (ICCCN), Munich, Germany, **(2012)** July 30-August 2.

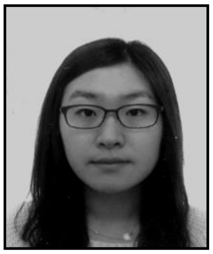
[7] T. Kothmayr, C. Shmitt, W. Hu, M. Brunig and G. Carle, “A DTLS Based End-To-End Security Architecture for the Internet of Things with Two-Way Authentication”, Proceedings of the 37th Conference on Local Computer Networks Workshops, Clearwater, Florida, USA, **(2012)** October 22-25.

[8] Tinydtls Documentation, http://tinydtls.sourceforge.net/.

[9] O. Bergmann, S. Gerdes and C. Bormann, “Simple Keys for Simple Smart Objects”, Proceedings of Workshop on Smart Object Security, Paris, France, **(2012)** March 23.

[10] R. Hummen, J. Ziegeldorf, H. Shafagh, S. Raza and K. Wehrle, “Towards Viable certificate-based Authentication for the Internet of Things”, Proceedings of the 2st ACM workshop on Hot topics on wireless network security and privacy, Budapest, Hungary, **(2013)** April 19.

Authors



Jiye Park, she received Bachelor's degree in computer system from Duksung Women's University, Korea in 2013. After obtaining Bachelor's degree, she is working towards master's degree in network security from Duksung Women's University. Her research interests include Internet of Things (IoT) and Web of Things (WoT). Especially, she is interested in Security in IoT and WoT.

Namhi Kang, he received B.E. and M.S. degrees in electrical and communications engineering from Soongsil University, Korea in 1999 and 2001, respectively. He received a Ph.D. degree in information and communications engineering from Siegen University, Germany, in December 2004. In 2005 he joined Ubiquitous Network Research Center, DASAN Networks, where he was a senior engineer. Since 2009, he has been a professor in the Department of Digital Media, Duksung Women's University in Seoul Korea. His research interests include network technology and security in wired and wireless networks, and the design of communication protocols for future oriented networks.